JAPAN SMARTPHONE SECURITY ASSOCIATION

第2回

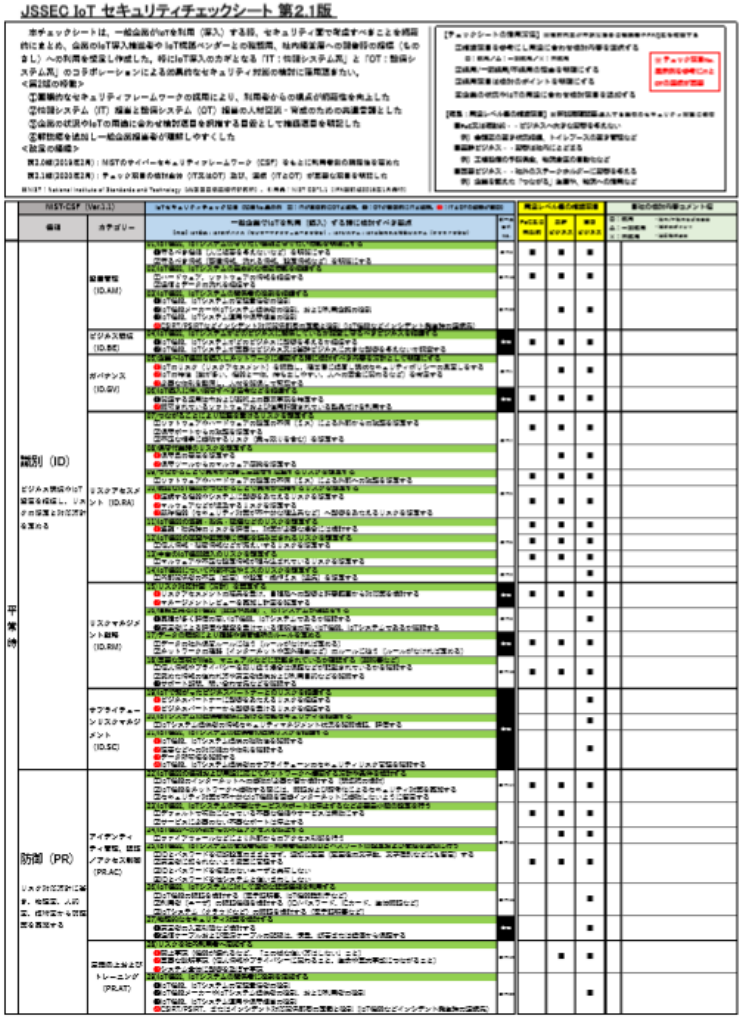
チェックシートの特徴と セキュリティの重要性

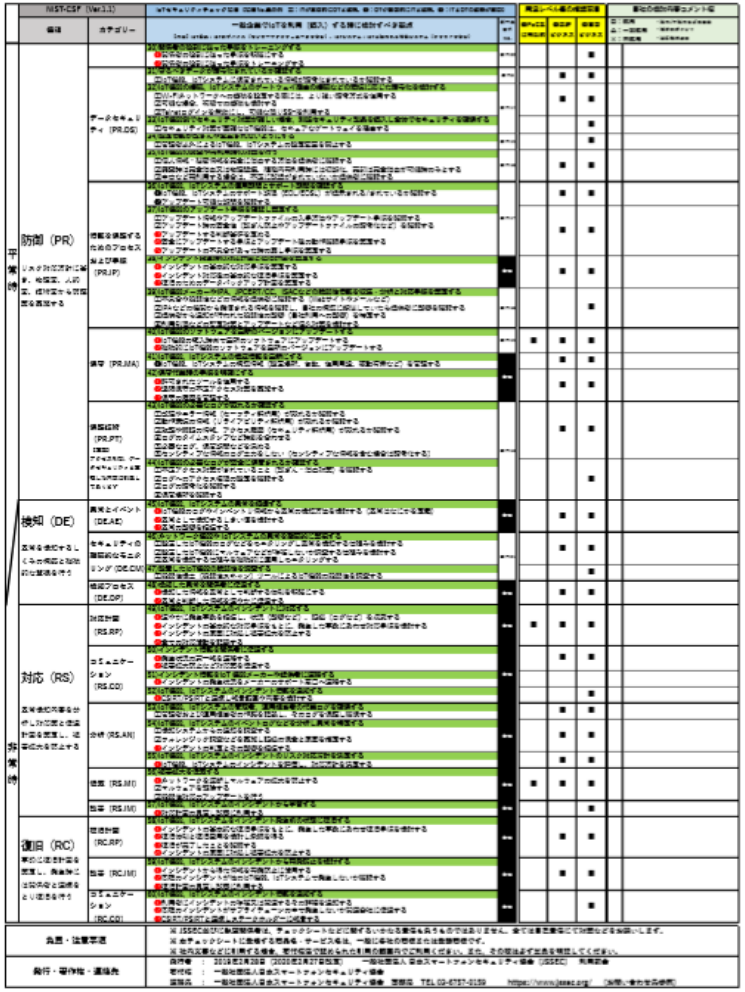
～安心・安全にIoTを活用するために～

2020年9月1日
日本スマートフォンセキュリティ協会 （JSSEC）
利用部会　IoT調査・研究TF
部会長 後藤 悦夫（株式会社 ラック）

IoTセキュリティチェックシート

JAPAN SMARTPHONE SECURITY ASSOCIATION


JSSEC IoT セキュリティチェックシート 第2.1版



チェックシートの特徴

JAPAN SMARTPHONE SECURITY ASSOCIATION

❶NIST-CSFの分類：5機能 23カテゴリー（識別/防御/検知/対応/復旧）
❷企業のIoT推進者や管理者の視点で検討すべき点：60項目
❸IoT用途レベル毎の推奨項目：3つの重要度に分類
❹各社の検討内容　採用理由／追加項目：検討結果の見える化
❺検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

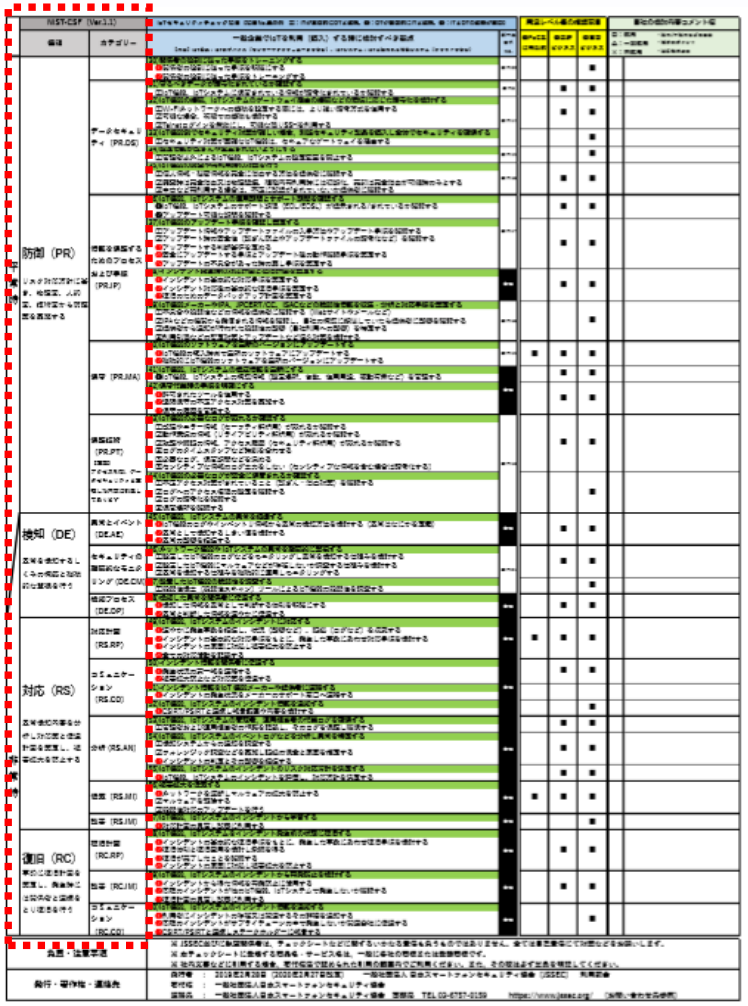
❶ ❺←2.1版 ❷ ❸ ❹

NIST-CSF（Ver.1.1）		IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】		用途レベル毎の推奨項目			自社の検討内容コメント欄
機能	カテゴリー	一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	IoC又は補助的	基幹ビジネス	重要ビジネス	■：採用　・採用/不採用などの理由 ■：一部採用　・検討のポイント ■：不採用　・追加検討項目
識別（ID）	資産管理（ID.AM）	01)IoT機器、IoTシステムの守りたい機能と守りたい情報を明確にする ❶守るべき機能（人に被害を与えないなど）を明確にする ②守るべき情報（蓄積情報、流れる情報、設定情報など）を明確にする	要点3	■	■	■	
		02)IoT機器、IoTシステムの基本的な構成情報を把握する ①ハードウェア、ソフトウェアの情報を把握する ②通信とデータの流れを把握する	要点18	■	■	■	
		03)IoT機器、IoTシステムの関係者の役割を把握する ❶IoT機器、IoTシステムの管理責任者の役割 ❷IoT機器メーカーやIoTシステム提供者の役割、および利用企業の役割 ❸IoT機器、IoTシステム運用や保守担当の役割 ❹CSIRT/PSIRTなどインシデント対応関係部署の定義と役割（IoT機器などインシデント発生時の連携先）	要点20		■	■	
	ビジネス環境（ID.BE）	04)IoT機器、IoTシステムがどのビジネスに関係しているか調査し守るべきビジネスを把握する ❶IoT機器、IoTシステムがどのビジネスに影響を与えるか把握する ❷IoT機器、IoTシステムが重要なビジネス又は基幹ビジネスに大きな影響を与えないか調査する	新規	■	■	■	
	ガバナンス（ID.GV）	05)企業へIoT機器を導入しネットワークに接続する時に検討すべき内容を方針として明確にする ❶IoTのリスク（リスクアセスメント）を認識し、経営層に提言し現状セキュリティポリシーの見直しをする ❷IoTの特性（数が多い、機器と一体、持ち出しやすい、人への安全に関わるなど）を考慮する ❸必要な体制を整備し、人材を確保して育成する	要点1		■	■	
		06)IoT導入に伴い順守すべき法令などを把握する ❶関連する適用法令および契約上の要求事項を特定する ❷認可されているソフトウェアおよび使用許諾されている製品だけを利用する	新規	■	■	■	
		07)つながることにより攻撃を受けるリスクを想定する ①ソフトウェアやハードウェアの設定の不備（ミス）による外部からの攻撃を想定する ②保守ポートからの攻撃を想定する ③不正な相手に接続するリスク（乗っ取りを含む）を想定する	要点4	■	■	■	
		08)保守作業時のリスクを想定する ❶保守員の悪意を想定する ❷保守ツールからのマルウェア感染を想定する			■	■	
		09)つながることで異常が伝播し意図せず攻撃するリスクを想定する ①ソフトウェアやハードウェアの設定の不備（ミス）による外部からの攻撃を想定する		■	■	■	

NIST-CSFの分類

JAPAN SMARTPHONE SECURITY ASSOCIATION

特徴❶



NIST-CSFとは

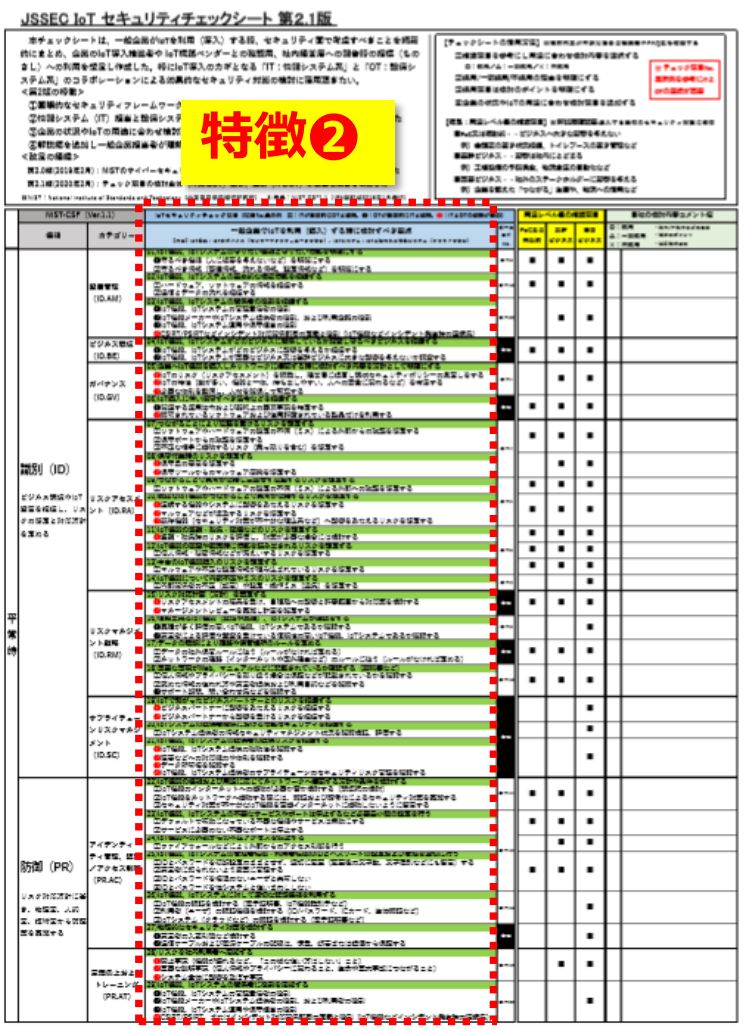
JAPAN SMARTPHONE SECURITY ASSOCIATION

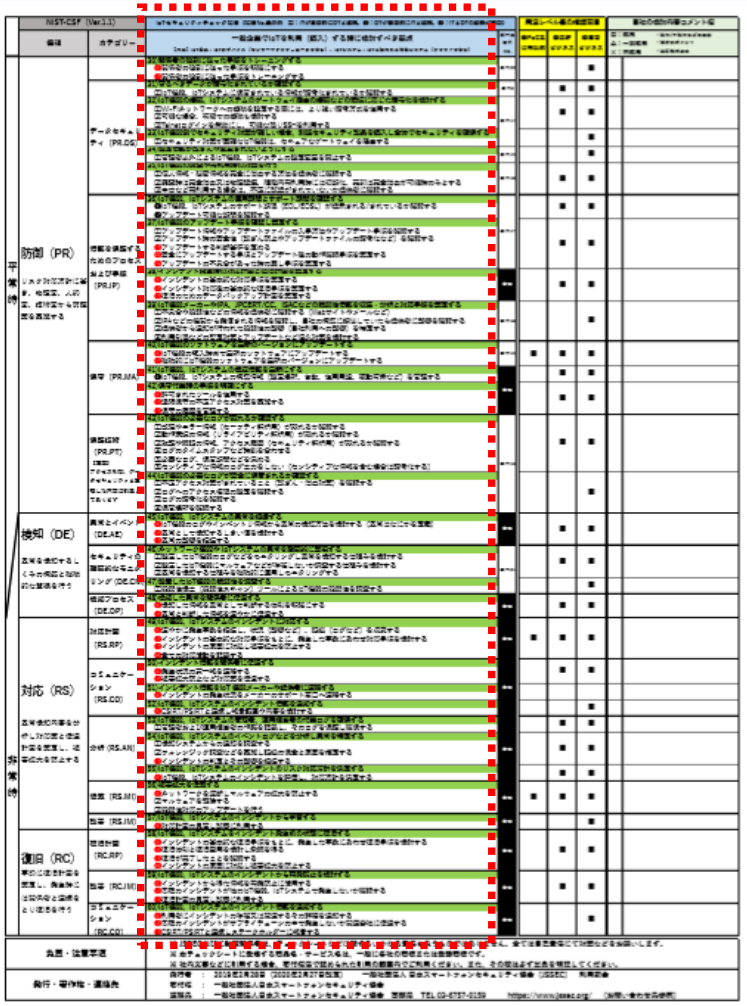
NISTのCSF：サイバーセキュリティフレームワーク

NIST : National Institute of Standards and Technology
（米国国立標準研究所）
CSF : Cyber Security Framework
➔ 汎用的なフレームワーク
世界各国が準拠を進めている

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

利用する視点で検討すべき点





一般企業のIoT利用シーンとは

JAPAN SMARTPHONE SECURITY ASSOCIATION

一般企業のIoT利用 ＝ 企業のスマート化

「Society 5.0」＝　超スマート社会（新たな付加価値の創出）

「Connected Industries」＝　日本版・第四次産業革命

①サイバー空間とフィジカル空間が高度に融合した産業社会

②コアテクノロジーはIoTを起点にビックデータやAIとの連携

➔サイバー・フィジカル・セキュリティ対策フレームワーク

「企業のスマート化」

①スマートOO（工場、物流、ショップ、オフィス）

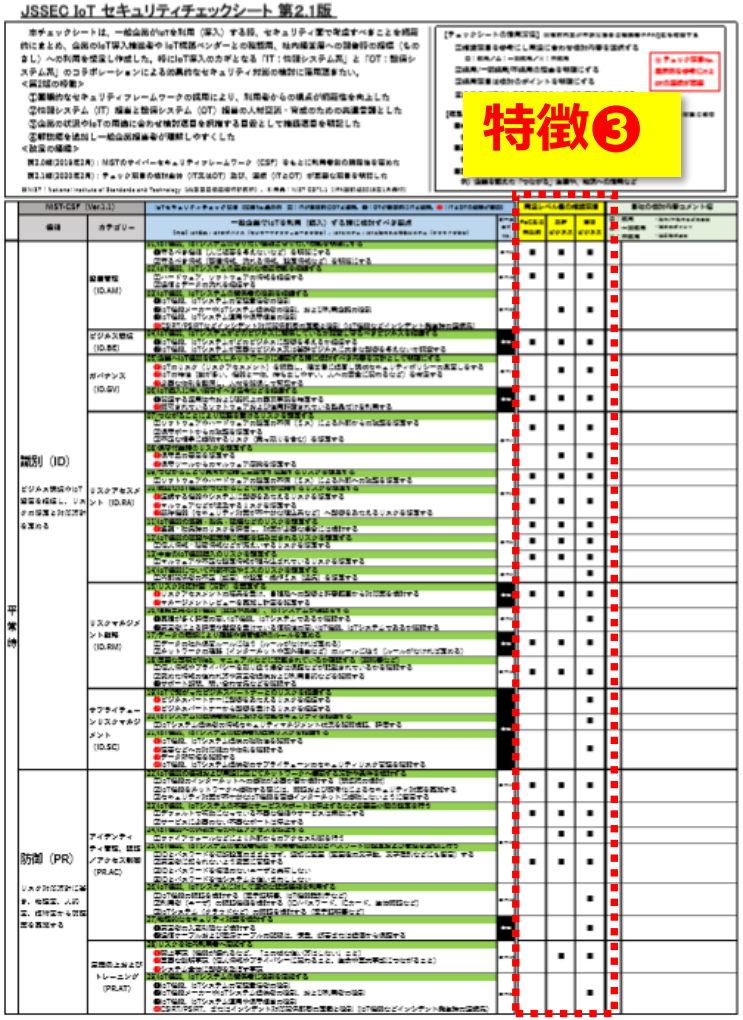
②コアテクノロジーはIoT

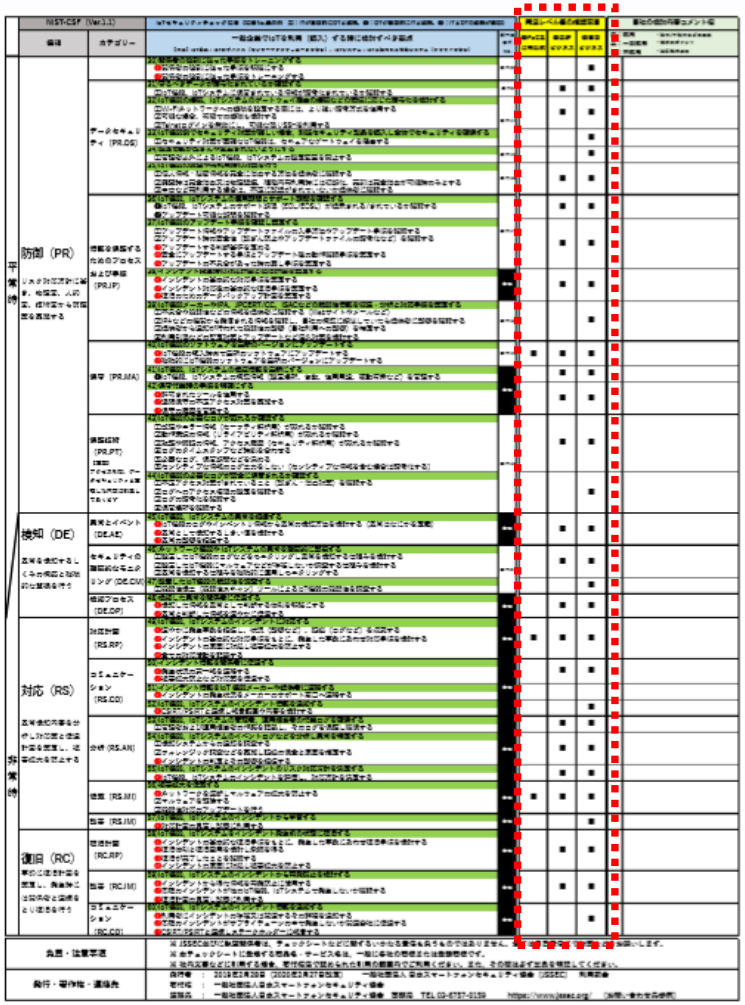
➔ IoTを安心・安全に活用するため、IoTセキュリティの共通的な検討項目を洗い出しを行った！

＝「IoTセキュリティチェックシート」

用途レベルに合わせ選択と追加

JAPAN SMARTPHONE SECURITY ASSOCIATION





用途レベルに合わせた選択と追加

JAPAN SMARTPHONE SECURITY ASSOCIATION

③ 用途レベル毎の推奨項目

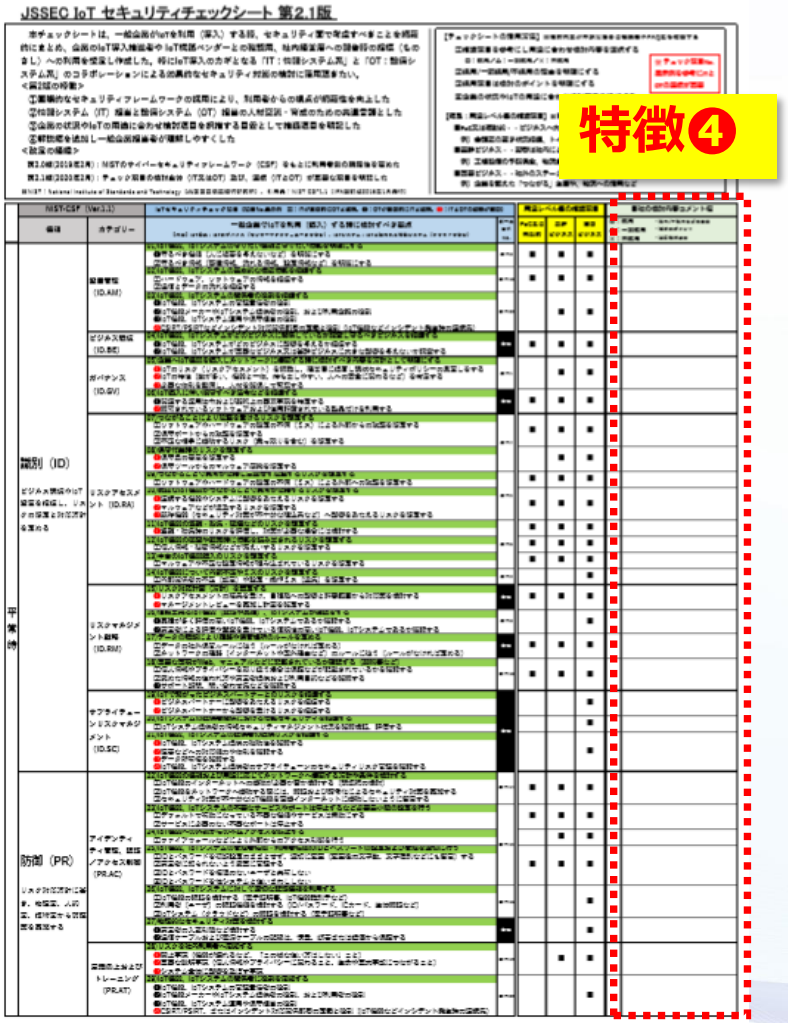
❶PoC又は補助的・・ビジネスへ大きな影響を与えない
例）会議室の空き状況把握、トイレブースの空き管理など

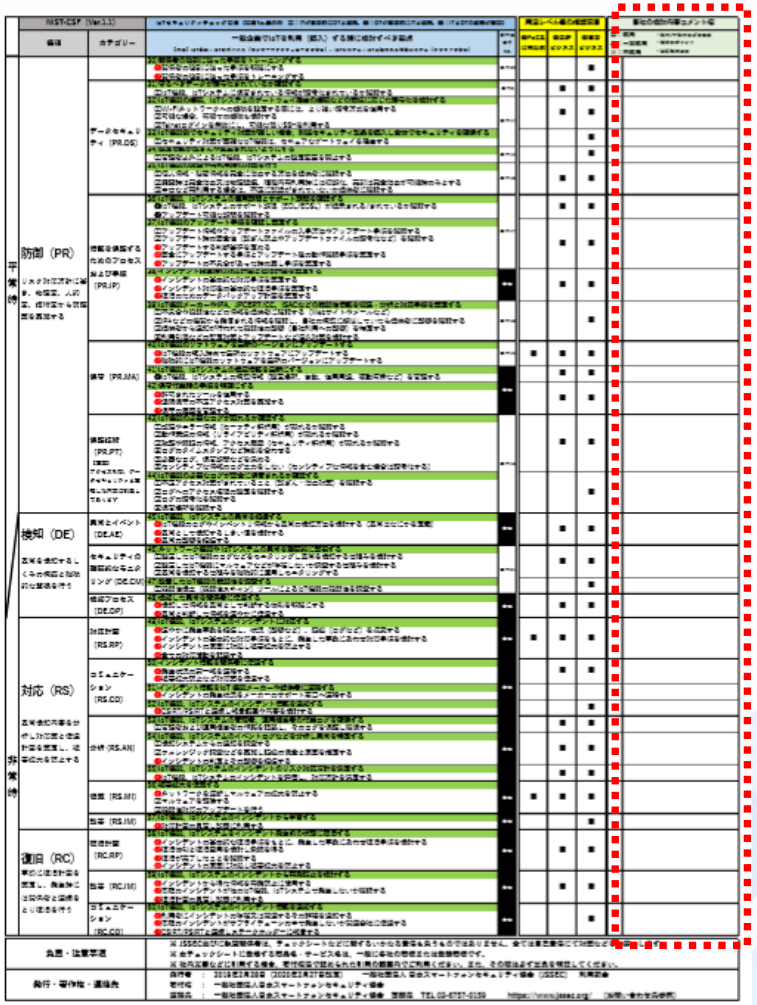
❷基幹ビジネス・・影響は社内にとどまる
例）工場設備の予防保全、物流倉庫の自動化など

❸重要ビジネス・・社外のステークホルダーに影響を与える
例）企業を超えた「つながる」生産や、物流への活用など

各社の検討結果の見える化

JAPAN SMARTPHONE SECURITY ASSOCIATION





各社の検討結果の見える化

JAPAN SMARTPHONE SECURITY ASSOCIATION

④ 自社の検討内容コメント欄 （活用はEXCELでセル拡大）

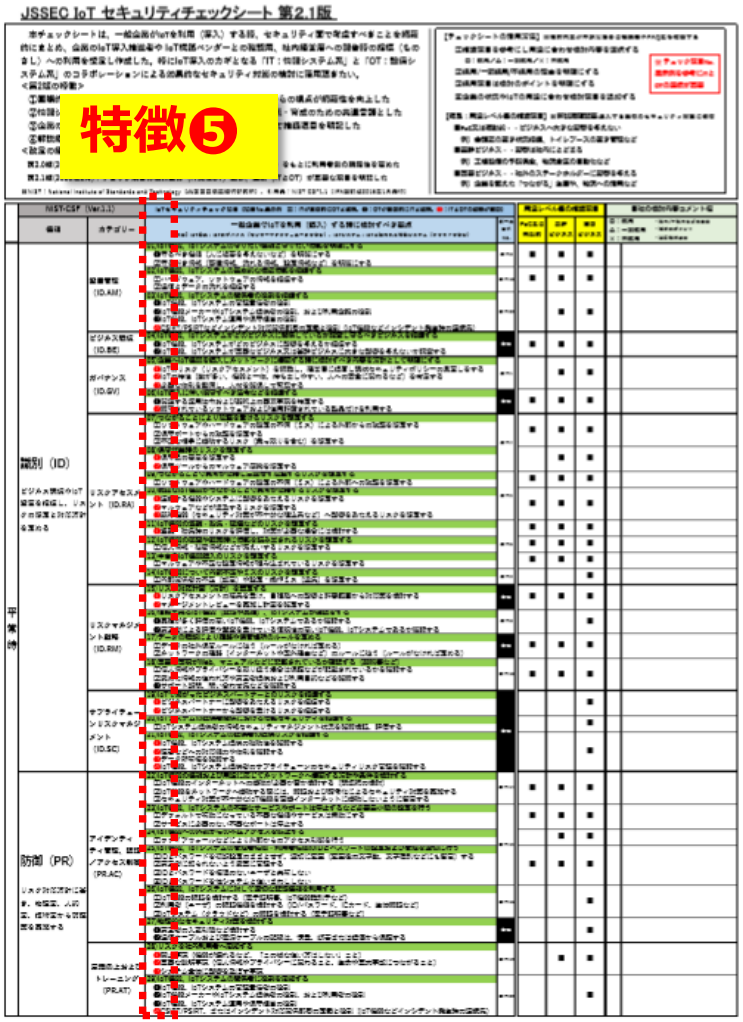
➔ IoTは長期間の利用を想定し、検討結果を継承することが重要

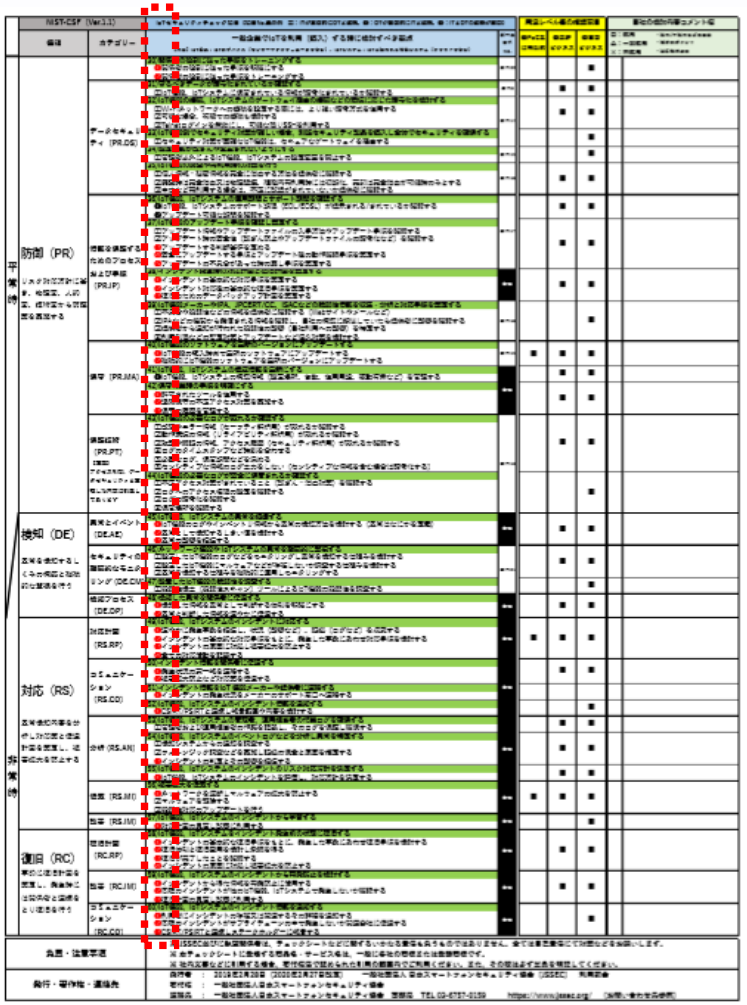
①「◎」採用/「△」一部採用/「×」不採用の理由を明確にする
②採用項目は検討のポイントを明確にする
③企業の状況やIoTの用途に合わせ検討項目を追加する

JSSEC IoT セキュリティチェックシート 第2.1版（用途レベル毎の推奨項目のPoC又は補助的のみ）

検討主体や連携が重要な項目

JAPAN SMARTPHONE SECURITY ASSOCIATION





検討主体や連携が重要な項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

■第2.1版(2020年2月)改訂のポイント

ねらい → ITとOTの連携をよりスムーズに進めるために

チェック項目の検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記した。　**※項目No.表示を色分けし明記**

①：ITが主体的　・・・・・情報セキュリティや情報技術
❶：OTが主体的　・・・・・新たにIoTとして検討が必要
❶：ITとOTの連携が重要　・効果的なセキュリティ対策のカギ

【注意】

・主体的とは連携が必要となるが**リードする側**を表す
・連携とは**互いに議論**するなど密に連携が重要な項目を表す

チェックシートを活用する企業の体制により主体や連携すべき項目は変わってくる、**検討をはじめる段階で連携の方法や項目を議論する事を推奨する**

IoTセキュリティの重要性

JAPAN SMARTPHONE SECURITY ASSOCIATION

■セキュリティインシデントの事例（2016年）

■日本の監視カメラ6000台もの映像が見られてる

➔ロシアのウェブサイトに公開

世界120か国の**監視カメラの映像をリアルタイムで見られてしまう！**

日本国内の監視カメラもおよそ6000か所、
デパート、歯医者、ホテルなど顔がくっきり映っていた。

原因は、**「購入時に初期パスワードを変更せず」**使っていた。

出典：ITmedia（2016）

■日本の防犯カメラも1000台以上リアルタイムで盗み見可能

➔ 2020年7月　出典：Gigazine（https://gigazine.net/news/20200718-insecam/）

IoTセキュリティの重要性

JAPAN SMARTPHONE SECURITY ASSOCIATION

■情報セキュリティとIoTセキュリティの違い
➔ サイバー空間とフィジカル空間の融合に注意

❶モノがつぶやく
・自分の情報（位置、活動、画像など）が集められる
◎求められる事 ➔ Privacy by Design

❷ネットを通じモノが制御される
・機密を守るから動作（制御）を守る
◎求められる事 ➔ Security by Design

❸長く使われる/モノが進化する
・スマホは3～5年、車や設備系は10年以上
◎求められる事 ➔ 長期的なアップデート

❹多種多様な使われ方
・使う人、管理する人がセキュリティをあまり意識しない
◎求められる事 ➔ ユーザーへの啓発やサポート

「識別」の概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ビジネス環境やIoT資産を把握し、**リスクの想定と対応方針**を定める
- **識別は用途レベルに関らず**、実施することを推奨（防御のベース）
- **踏み台にならないための**、リスク想定が重要
- **サプライチェーンリスク**（ビジネスパートナー、提供者）

NIST-CSF（Ver.1.1）		IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】	
機能	カテゴリー	一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版 要点 No.
識別（ID）	資産管理（ID.AM）	01)IoT機器、IoTシステムの守りたい機能と守りたい情報を明確にする	要点3
		02)IoT機器、IoTシステムの基本的な構成情報を把握する	要点18
		03)IoT機器、IoTシステムの関係者の役割を把握する	要点20
	ビジネス環境（ID.BE）	04)IoT機器、IoTシステムがどのビジネスに関係しているか調査し守るべきビジネスを把握する	新規
	ガバナンス（ID.GV）	05)企業へIoT機器を導入しネットワークに接続する時に検討すべき内容を方針として明確にする	要点1
		06)IoT導入に伴い順守すべき法令などを把握する	新規
	リスクアセスメント（ID.RA）	07)つながることにより攻撃を受けるリスクを想定する	要点4
		08)保守作業時のリスクを想定する	
		09)つながることで異常が伝播し意図せず攻撃するリスクを想定する	要点5
		10)脆弱なIoT機器がつながることで異常が伝播するリスクを想定する	
		11)IoT機器の盗難・紛失・破壊などのリスクを想定する	要点6
		12)IoT機器の破棄や転売時に情報を読み出されるリスクを想定する	
		13)中古のIoT機器購入のリスクを想定する	
		14)IoT機器について内部不正やミスのリスクを想定する	要点2
	リスクマネジメント戦略（ID.RM）	15)リスク対応計画（方針）を策定する	新規
		16)信頼出来るIoT機器（認証や実績）、IoTシステムか確認をする	要点3
		17)データの種類により経路や保管場所のルールを定める	新規
		18)重要な事項がWeb、マニュアルなどに記載されているか確認する（契約書など）	要点18
	サプライチェーンリスクマネジメント（ID.SC）	19)IoTで繋がったビジネスパートナーとのリスクを把握する	新規
		20)IoTシステムの提供者関係における情報セキュリティを把握する	
		21)IoT機器、IoTシステムの提供者の提供リスクを把握する	

「防御」の概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

■リスク対応方針に基き、**物理面、人的面、技術面から防護策**を実施する

- **防御は用途レベルにあわせ**、対策を検討することが重要
- **IoTは使用期間が長い**、サポート期間の確認も重要

NIST-CSF（Ver.1.1）		IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】	
機能	カテゴリー	一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.
防御（PR）	アイデンティティ管理、認証／アクセス制御（PR.AC）	22)IoT機器の機能および用途に応じてネットワークへ接続する方針や条件を検討する	要点14
		23)IoT機器、IoTシステムの不要なサービスやポートは停止するなど必要最小限の設定を行う 24)IoT機器への外部からの不正アクセスを防止する 25)IoT機器、IoTシステムの管理者権限・利用者権限のIDとパスワードの設定および管理を適切に行う	要点15
		26)IoT機器、IoTシステムに対して適切な認証機能を利用する	要点16
		27)物理的なセキュリティ対策を検討する	新規
	意識向上トレーニング（PR.AT）	28)リスクを社内利用者へ周知する	要点19
		29)IoT機器、IoTシステムの関係者に役割を周知する	要点20
		30)関係者の役割に従った手順をトレーニングする	要点20
	データセキュリティ（PR.DS）	31)守るべきデータが暗号化されているか確認する	要点8
		32)IoT機器の接続、IoTシステムのゲートウェイ経由の接続などの環境に応じた暗号化を検討する	要点14
		33)IoT機器側でセキュリティ対策が難しい場合、別途セキュリティ製品を導入し全体でセキュリティを確保する 34)設定情報が改ざんや変更されないようにする	要点15
		35)IoT機器の廃棄や再利用時の対策を行う	要点18
	情報を保護するためのプロセスおよび手順（PR.IP）	36)IoT機器、IoTシステムの使用期間とサポート期間を確認する	要点17
		37)IoT機器のアップデート手順を確認し策定する	
		38)インシデント発生時の対応計画と復旧計画を策定する	新規
		39)IoT機器メーカーやIPA、JPCERT/CC、ISACなどの脆弱性情報を収集・分析と対応手順を策定する	要点18
	保守（PR.MA）	40)IoT機器のソフトウェアを最新のバージョンにアップデートする	要点15
		41)IoT機器、IoTシステムの構成情報を最新にする 42)保守作業時の手順を明確にする	新規
	保護技術（PR.PT）	43)IoT機器の必要なログが取れるか確認する 44)IoT機器の必要なログが安全に保管されるか確認する	要点13

「検知・対応・復旧」の概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

検知（DE）：**異常を検知**するしくみの構築と継続的な監視を行う

対応（RS）：異常検知の内容を分析し対応策と伝達計画を策定し、**被害拡大を防止**する

復旧（RC）：事前に復旧計画を策定し、発生時には**関係者と連携**をとり復旧を行う

NIST-CSF（Ver.1.1）		IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】	
機能	カテゴリー	一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.
検知（DE）	異常とイベント（DE.AE）	45)IoT機器、IoTシステムの異常を把握する	新規
	モニタリング（DE.CM）	46)ネットワーク機器やIoTシステムの異常を継続的に監視する 47)設置したIoT機器の脆弱性を調査する	要点21
	検知プロセス（DE.DP）	48)検知した異常を関係者に伝達する	新規
対応（RS）	対応計画（RS.RP）	49)IoT機器、IoTシステムのインシデントに対応する	新規
	コミュニケーション（RS.CO）	50)インシデント情報を関係者に伝達する	
		51)インシデント情報をIoT機器メーカーや提供者に連絡する	新規
		52)IoT機器、IoTシステムのインシデント情報を通知する	
	分析（RS.AN）	53)IoT機器、IoTシステムの管理者、運用担当者の作業ログを確保する 54)IoT機器、IoTシステムのイベントログなどを分析し異常を特定する 55)IoT機器、IoTシステムのインシデントのリスク対応方針を決定する	新規
	低減（RS.MI）	56)被害拡大を低減する	新規
	改善（RS.IM）	57)IoT機器、IoTシステムのインシデントから学習する	新規
復旧（RC）	復旧計画（RC.RP）	58)IoT機器、IoTシステムをインシデント発生前の状態に復旧する	新規
	改善（RC.IM）	59)IoT機器、IoTシステムのインシデントから再発防止を検討する	新規
	コミュニケーション	60)IoT機器、IoTシステムのインシデント情報を通知する	新規

チェックシート活用のイメージ

JAPAN SMARTPHONE SECURITY ASSOCIATION

本チェックシートは、一般企業がIoTを利用（導入）する時、
セキュリティ面で考慮すべきことを網羅的にまとめています。

◆想定する活用イメージ：
- 社内IoT導入推進者の検討のベース
- 社内の経営層などへの報告時の指標（ものさし）
- IoT構築ベンダーとの確認用

特に安心・安全なIoT導入のカギとなる
「IT：情報システム系」と「OT：設備システム系」
のコラボレーションによる、
効果的なセキュリティ対策の検討に活用頂きたい。

次回の紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

■IoTセキュリティチェックシート入門

■次回にはチェック項目「識別」になります。
ぜひ次回の③をご覧頂き、IoTセキュリティの「具体的」な取り組み方を感じて頂ければ幸いです。

③識別（各項目の概要）

■識別は検討の出発点で「ビジネス環境やIoT資産を把握し、**リスクの想定と対応方針を定める**」の項目を紹介します。

■関係者が**現状を共有することが重要**です。

次回の受講おまちしております。